**EXHIBIT 3**

CHRISTOPHER GRIVAKES
cg@agzlaw.com
DAMION ROBINSON
dr@agzlaw.com
AFFELD GRIVAKES LLP
2049 Century Park East, Suite 2460
Los Angeles, CA 90067
Telephone: 310.979.8700
Facsimile: 310.979.8701

Attorneys for Plaintiff ROBERT ROSS

THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ROBERT ROSS,

Plaintiff,

v.

AT&T MOBILITY, LLC, ONE TOUCH DIRECT, LLC, and ONE TOUCH DIRECT- SAN ANTONIO, LLC,

Defendants.

Case No. 3:19-cv-6669

**FIRST AMENDED COMPLAINT**

**DEMAND FOR JURY TRIAL**

## I. NATURE OF THE ACTION

1. This action arises out of AT&T's failure to protect the sensitive and confidential account data of its mobile service subscriber, Robert Ross, resulting in massive violations of Mr. Ross's privacy, the compromise of his highly sensitive personal and financial information, and the theft of more than $1 million.

2. AT&T is the country's largest mobile service provider. Tens of millions of subscribers entrust AT&T with access to their confidential information, including information that can serve as a key to unlock subscribers' highly sensitive personal and financial information.

3. Recognizing the harms that arise when mobile subscribers' personal information is accessed, disclosed, or used without their consent, federal and state laws require AT&T to protect this sensitive information.

4. AT&T also recognizes the sensitivity of this data and promises its subscribers that it "will protect [customers'] privacy and keep [their] personal information safe" and that it "will not sell [customers'] personal information to anyone, for any purpose. Period." AT&T repeatedly broke these promises.

5. In an egregious violation of the law and its own promises, and despite advertising itself as a leader in technological development and as a cyber security-savvy company, AT&T breached its duty and promise to Mr. Ross to protect his account and the sensitive data it contained. AT&T failed to implement sufficient data security systems and procedures, instead allowing third parties to gain unauthorized access to Mr. Ross's AT&T account in order to steal from him.

6. AT&T's actions and conduct were a substantial factor in causing significant financial and emotional harm to Mr. Ross and his family. But for AT&T employees', representatives' and agents' unauthorized access to Mr. Ross' account, and failure to protect Mr. Ross through adequate security and oversight systems and procedures, Mr. Ross would not have had his personal privacy repeatedly violated and would not have been a victim of SIM swap theft.

7. Mr. Ross brings this action to hold AT&T accountable for its violations of federal and state law, and to recover for the grave financial and personal harm suffered by Mr. Ross and his family as a direct result of AT&T's acts and omissions, as detailed herein.

## II. THE PARTIES

8. Plaintiff Robert Ross is, and at all relevant times was, a resident of California. Mr. Ross currently resides in San Francisco, California.

9. Mr. Ross was an AT&T mobile customer at all times relevant to this Complaint. He purchased a mobile phone plan from AT&T in San Francisco, California in 2007 for personal use, was an active, paying AT&T mobile subscriber at all times relevant to the allegations in this Complaint, and his business relationship was directly with AT&T at all relevant times.

10. Defendant AT&T Mobility, LLC (hereinafter, "AT&T") is a Delaware limited liability corporation with its principal office or place of business in Brookhaven, Georgia. AT&T "provides nationwide wireless services to consumers and wholesale and resale wireless subscribers located in the United States or U.S. territories" and transacts or has transacted business in this District and throughout the United States. It is the second largest wireless carrier in the United States, with more than 153 million subscribers, earning $71 billion in total operating revenues in 2017 and $71 billion in 2018. As of December 2017, AT&T had 1,470 retail locations in California.OF[1]

11. AT&T provides wireless service to subscribers in the United States. AT&T is a "common carrier" governed by the Federal Communications Act ("FCA"), 47 U.S.C. § 151 *et seq*. AT&T is regulated by the Federal Communications Commission ("FCC") for its acts and practices, including those occurring in this District.

[1] "About Us," AT&T, *available at* https://engage.att.com/california/about-us/. All URLs in this complaint were last accessed on October 15, 2019.

12. AT&T Inc., AT&T's parent company, acknowledged in its 2018 Annual Report that its "profits and cash flow are largely driven by [its] Mobility business" and "nearly half of [the] company's EBITDA (earnings before interest, taxes, depreciation and amortization) come from Mobility."1F[2]

13. Defendant One Touch Direct, LLC ("One-Touch Direct") is a Florida Corporation with its principal place of business in Tampa, Florida. Plaintiff is informed and believes and thereon alleges that AT&T contracted with One-Touch Direct to provide call center services for AT&T's mobile phone customers.

14. Defendant One Touch Direct - San Antonio, LLC ("One-Touch Direct-SA") is a Florida Corporation with its principal place of business in Tampa, Florida. Plaintiff is informed and believes and thereon alleges that One-Touch Direct-SA is a subsidiary of One Touch Direct - SA and the employer of the customer service representative(s) who executed the remote SIM swap on Plaintiff's mobile phone.

15. At all relevant times, One Touch Direct and One Touch Direct-SA were AT&T's authorized representatives and agents and performed services for AT&T which were within the usual course of AT&T's business.

16. At all relevant times, AT&T dictated and controlled the manner and means by which One Touch Direct and One Touch Direct-SA performed their services for AT&T. On information and belief, AT&T entered into a master service agreement with One Touch Direct which governed the terms and condition of AT&T's relationship with One Touch Direct and its subsidiaries such as One Touch Direct-SA, and which required the One Touch entities to strictly adhere to AT&T's guidelines, protocols, policies, and procedures relating to customer service, including those relating to SIM swaps. Furthermore, AT&T controlled the security measures it implemented across its entire network operation (including its

[2] *Id.*

own call centers and third party call centers), as well as the data accumulated across the entire network, to monitor, detect and prevent unauthorized SIM swaps.

17. At all relevant times, One Touch Direct and One Touch Direct-SA employees identified themselves to Mr. Ross as "AT&T" rather than One Touch Direct (at AT&T's direction), had full access to and use of the AT&T customer database which enabled them to perform customer service functions (including SIM swaps), did not disclose that they were employed by One Touch Direct, and were in essence *de facto* employees of AT&T.

## III. JURISDICTION AND VENUE

18. This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ("FCA"). The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts. The Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1332 because Mr. Ross is a citizen of a different state than AT&T, One Touch Direct, and One Touch Direct-SA.

19. This Court has personal jurisdiction over AT&T and its contractors One Touch Direct and One Touch Direct-SA because AT&T purposefully directs its conduct at California, transacts substantial business in California (including in this District), has substantial aggregate contacts with California (including in this District), engaged and is engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in California (including in this District), and purposely avails itself of the laws of California. AT&T had more than 33,000 employees in California as of 2017, and 1,470 retail locations in the state.2F[3] Mr. Ross purchased his AT&T mobile plan in California, visited AT&T retail locations in California, and was injured in California by the acts and omissions alleged herein.

[3] "About Us," AT&T California, *supra* at 1.

20. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Mr. Ross' claims occurred in this District and Defendant transacts business in this District. Mr. Ross purchased his AT&T mobile plan in this District and was harmed in this District, where he resides, by the acts and omissions of Defendants, as detailed herein.

## IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

21. As a telecommunications carrier, AT&T is entrusted with the sensitives mobile account information and personal data of millions of Americans, including Mr. Ross' confidential and sensitive personal and account information. AT&T's duties to safeguard customer information are non-delegable to any other entity, including its third-party call center service providers such as One Touch Direct.

22. Despite its representations to its customers and its obligations under the law, AT&T has failed to protect Mr. Ross' confidential information. In October 2018, AT&T employees, representatives and agents obtained unauthorized access to Mr. Ross' AT&T mobile account, viewed his confidential and proprietary personal information, and transferred control over Mr. Ross' AT&T mobile number and service from Mr. Ross' phone to a phone controlled by third-party hackers. The hackers then immediately utilized their control over Mr. Ross' AT&T mobile number—control secured with necessary and direct assistance from AT&T employees, representatives and agents —to access his personal and digital finance accounts and steal $1 million from Mr. Ross.

23. This type of telecommunications account hacking behavior is known as "SIM swapping."

### A. SIM Swapping is a Type of Identity Theft Involving the Transfer of a Mobile Phone Number

24. Mr. Ross was the target of a "SIM swap" on October 26, 2018.

25. "SIM swapping" refers to a relatively simple scheme, wherein third parties take control of a victim's mobile phone number. The hackers then use that phone number as a key to access and take over the victim's digital accounts, such as email, file storage, and financial accounts.

26. Most mobile phones, including the iPhone owned by Mr. Ross at the time of his SIM swap, have an internal SIM ("subscriber identity module") card. A SIM card is a small, removable chip that allows a mobile phone to communicate with the mobile carrier's network and the carrier to know what subscriber account is associated with that mobile phone. The connection between the mobile phone and the SIM card is made through the carrier, which associates each SIM card with the physical phone's IMEI ("international mobile equipment identity"), which is akin to the mobile phone's serial number. Without an activated SIM card and effective SIM connection, a mobile phone typically cannot send or receive calls or text messages over the carrier network. SIM cards can also store a limited amount of account data, including contacts, text messages, and carrier information, and that data can help identify the subscriber.

27. The SIM card associated with a mobile phone can be changed. If a carrier customer buys a new phone that requires a different sized SIM card, for example, the customer can associate his or her account with a new SIM card and the new phone's IMEI by working with their mobile carrier to effectuate the change. This allows carrier customers to move their mobile number from one mobile phone to another and to continue accessing the carrier network when they switch mobile phones. For a SIM card change to be effective, the carrier is required by law to authenticate that the change request is legitimate and actualize the change. AT&T allows its employees, representatives and agents to conduct SIM card changes for its customers remotely or in its retail stores, and does so numerous times daily with inadequate protections against unauthorized SIM swaps.

28. An unauthorized SIM swap refers to an illegitimate SIM card change. During a SIM swap attack, the SIM card number associated with the victim's mobile account is switched from the victim's phone to a phone controlled by a third party. This literally re-routes the victim's mobile phone service — including any incoming data, texts, and phone calls associated with the victim's phone — from the victim's physical phone to a physical phone controlled by the third party (also referred to herein as a "hacker"). The hacker's phone then becomes the phone associated with the victim's carrier account, and the hacker receives all of the text messages and phone calls intended for the victim.3F[4] Meanwhile, the victim's mobile phone loses its ability to connect to the carrier network.

29. Once hackers have control over the victim's phone number, they can immediately use that control to access and take complete control of the victim's personal online accounts, such as email and banking accounts, through exploiting password reset links and codes sent via text message to the now-hacker-controlled-phone or the two-factor authentication processes associated with the victim's digital accounts. Two-factor authentication allows digital accounts to be accessed without a password or allows the account password to be changed. One common form of two-factor authentication enabled, allowed, and used by AT&T itself is through text messaging. Rather than enter a password, the hacker requests that a password reset link or code be sent to the mobile phone number associated with the victim's online account which AT&T makes possible. Because the hacker now controls the victim's phone number, the reset code is sent to the hacker. The hacker can then log into, and change the password for, the victim's account,

[4] As described by federal authorities in prosecuting SIM swap cases, SIM swapping enables hackers to "gain control of a victim's mobile phone number by linking that number to a subscriber identity module ('SIM') card controlled by [the hackers]—resulting in the victim's phone calls and short message service ('SMS') messages being routed to a device controlled by [a hacker]." *United States of America v. Conor Freeman, et al.*, No. 2:19-cr-20246-DPH-APP (E.D. Mich. Filed Apr. 18, 2019) (hereafter, "Freeman Indictment") (attached hereto as Exhibit A), ECF. No. 1 at ¶ 3.

allowing the hacker to access and take complete control of the contents of the account.4F[5]

30. Therefore, obtaining access to and control over a victim's mobile phone service is the central part of breaking into the victim's other online accounts, such as email services or financial accounts.

31. The involvement of a SIM swap victim's mobile carrier is critical to an unauthorized SIM swap. In order for an unauthorized SIM swap to occur and for a SIM swap victim to be at any risk, the carrier must activate the SIM card in the hacker's phone, which simultaneously results in the SIM card in the victim's phone to be deactivated. At that point, the victim's phone will display "No Service" as their phone can no longer connect to the carrier's network.

32. Upon information and belief, in Mr. Ross's case, not only did AT&T employees,representatives and agents access his account without authorization, they also changed his SIM card number to a phone controlled by hackers, who then immediately used that control to steal from Mr. Ross and access sensitive personal information.

**B. AT&T Allowed Unauthorized Access to Mr. Ross' AT&T Account**

33. AT&T representatives and agents accessed Mr. Ross' AT&T mobile account without his authorization, obtained his confidential and proprietary personal information, and gave complete control of his mobile service to hackers – all without Mr. Ross' knowledge or consent. Those hackers then immediately used their control over Mr. Ross' mobile phone number to access and take control of his sensitive and confidential information and accounts and steal more than $1 million

[5] *See, e.g.*, *Id.* at ¶ 4 ("Once [hackers] had control of a victim's phone number, it was leveraged as a gateway to gain control of online accounts such as the victim's email, cloud storage, and cryptocurrency exchange accounts. Sometimes this was achieved by requesting a password-reset link be sent via [text messaging] to the device control by [hackers]. Sometimes passwords were compromised by other means, and [the hacker's] device was used to received two-factor authentication ('2FA') message sent via [text message] intended for the victim.").

from him and access sensitive personal information such as passports, drivers' licenses and birth certificates.

34. On October 26, 2018 at approximately 6:00 PM PT, Mr. Ross began receiving notifications that someone was attempting to withdraw currency from his account at Gemini, a provider of financial services. This caused Mr. Ross significant distress because, at the time, Mr. Ross had $500,000 in USD in his Gemini account.

35. At approximately the same time, Mr. Ross noticed that his AT&T mobile phone had lost service and displayed "No Service", and he also noticed that he was automatically logged out of his Gmail account.

36. Mr. Ross immediately suspected that a hacker attack was underway and took his mobile phone to an Apple store for assistance.

37. Apple representatives assisted Mr. Ross in contacting AT&T Customer Support. At that time, an AT&T employee, representative and agent informed the Apple representatives that Mr. Ross' SIM card had been changed. AT&T employees, representatives and agents advised the Apple representatives to provide Mr. Ross with a new SIM card, and then Apple employees replaced the SIM card in Mr. Ross' phone. AT&T then activated the new SIM card, restoring Mr. Ross' access to his AT&T mobile number and account services.

38. When Mr. Ross returned home that evening, he called AT&T's customer service to discuss the unauthorized access to his account by AT&T employees, representatives and agents and the unauthorized SIM swap. An AT&T customer service representative who identified himself as Ryan S. (with a representative identification number RS410M) informed Mr. Ross that an unauthorized SIM swap had occurred on his service at approximately 5:47 PM PT by AT&T representative Cristelo V. (with a representative identification number CV921H).

39. AT&T representative Ryan S. also informed Mr. Ross that this unauthorized SIM swap request was made using customer owned and maintained equipment ("COAM"), and explained that COAM is a mobile phone that is not provided by AT&T and would generally be of unknown origin to AT&T (for example, a hacker might purchase a used mobile phone on the internet). Furthermore, Ryan S. expressed surprise that this SIM swap was executed as he told Mr. Ross it was against AT&T internal policies for an AT&T representative to execute a COAM-originated SIM swap request from anyone calling in to an AT&T call center. Ryan S further represented that he made a specific note of this violation of AT&T's own policy in Mr. Ross' account, reading the note verbally to Mr. Ross "I have informed customer that a SIM card and IMEI change occurred on 10/26/18 at 5:47pm. This change was approved by agent which is a direct violation of the ATT activation policy." After a couple of hours on this call, Ryan S told Mr. Ross that his supervisor would take over the call, which she did, and immediately told Mr. Ross that Ryan S should not have given the information he did to Mr. Ross, and she immediately and abruptly terminated the call, causing further distress to Mr. Ross.

40. AT&T employees, representatives and agents(including Ryan S.) represented to Mr. Ross that AT&T would place a warning on his account stating that he was experiencing fraud and instructing AT&T employees not to change anything on his account – including his SIM card.

41. AT&T informs its customers that verbal account passcodes—which are different than online account sign-in passwords or the passcodes used to access a mobile device—are used to protect customer's mobile accounts and may be required when a customer manages their AT&T account online or in an AT&T store.5F[6]

[6] "Get info on passcodes for mobile accounts," AT&T, *available at* https://www.att.com/esupport/article.html#!/mobile/KM1049472?gsi=tp3wtr.

42. Within minutes of AT&T giving control over Mr. Ross's AT&T mobile number to the hackers, they used that control to access and take over Mr. Ross' accounts at his financial services providers, including but not limited to, Coinbase, Gemini, and Binance. Coinbase and Gemini allow their users to store US dollars that can be used to buy and sell cryptocurrencies (such as bitcoin) within the user's account, in a similar way to how users can store US dollars used to buy and sell stocks at financial services providers such as Fidelity, Schwab, and E*Trade.

43. At the time of the SIM swap attack, Mr. Ross had approximately $500,000 in US dollars in his Gemini account and approximately $500,000 in US dollars in his Coinbase account. By utilizing their control over Mr. Ross' mobile phone number, which AT&T gave them, third-party hackers were able to access and take control of these accounts of Mr. Ross and control the entire USD amounts he held in both accounts. The hackers used Mr. Ross's $1,000,000 in US dollars to purchase bitcoin—a type of cryptocurrency that can be difficult to trace—and then the hackers transferred that bitcoin into accounts they controlled at a different financial services provider. This made the cryptocurrency exceedingly difficult to trace, let alone recover.[7]

44. The hackers also transferred cryptocurrency worth approximately $3,000 from Mr. Ross' Binance account into accounts they controlled, thereby stealing those funds from him as well.

45. The hackers also used their control over Mr. Ross' AT&T mobile phone number to access, change the passwords, and take control of several of Mr. Ross' most sensitive online accounts, including, but not limited to, his Authy, Google, Yahoo!, and DropBox accounts. In taking over his Google account, the

[7] *See* Investigation Report, Regional Enforcement Allied Computer Team, *California v. Nicholas Truglia* (Oct. 2018) (attached hereto as Exhibit B) at p. 8 ("explaining that "all of Robert R.'s funds stored in Coinbase (approximately $500,000) and Gemini (approximately $500,000) had been held in USD. The [hacker] used all the funds in USD at both exchanges to purchase bitcoins, then immediately withdrew all of the bitcoins. … This information was subsequently verified by obtaining records directly from Coinbase and Gemini via search warrant.").

hackers also changed his passwords and the phone number linked to Mr. Ross' two-factor authentication for these accounts, which made it impossible for Mr. Ross to regain immediate access to, let alone control of, these accounts (because any requests to remind him of or reset the password no longer were sent to Mr. Ross' mobile phone, but rather to the hacker's phone). It took Mr. Ross approximately 7-10 days to regain access to and restore control over his email and, and longer for his other online personal accounts, and several weeks to regain access to the accounts taken over at his other financial services providers. In addition, the hackers deleted several weeks-worth of emails and substantial data from Mr. Ross' Google account. Mr. Ross has not been able to recover any of this data.

46. Criminal investigations by the California-based Regional Enforcement Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement partnership specializing in cybercrime, into the October 2018 breach of Mr. Ross' AT&T account and the resulting theft revealed the involvement of a third-party hacker named Nicholas Truglia, who was arrested by REACT detectives on November 13, 2018, and faces 21 felony counts in Santa Clara County for SIM swaps and related thefts, including against Mr. Ross. In their investigation report, REACT detectives specifically wrote that they obtained a search warrant for AT&T records pertaining to these thefts, and in response, AT&T provided REACT investigators with records that showed the same mobile device used by the hacker (identified through the devices IMEI number) had been used to effect the account takeovers of Mr. Ross, as well as the accounts of several other victims. In total, the records indicated that, prior to the unauthorized and illegal SIM swap and theft facilitated by AT&T against Mr. Ross, 11 unique phone numbers had been SIM swapped using this device between October 5 and October 26, 2018. It is incredulous that AT&T not only allowed these other unauthorized SIM swaps to happen, resulting in several other victims, but certainly knew or should have

known that the same mobile device used to SIM swap other victims was already being used by a hacker who later used that same device to SIM swap Mr. Ross. Even the most basic check by AT&T would have easily flagged this IMEI as being used to perpetrate completely unauthorized and illicit SIM swaps well prior to the unauthorized and illegal SIM swap against Mr. Ross, which resulted within 45 minutes of the theft of almost his entire life's savings of $1,000,000.

47. Mr. Ross' financial and personal life have been uprooted as a result of AT&T's failure to safeguard his account.

48. As a result of the SIM swap detailed above, Mr. Ross lost more than $1 million in USD. This money constituted the majority of Mr. Ross' life savings and the money he had saved for his daughter's college fund as well as his own retirement.

49. The financial strain resulting from the robbery of Mr. Ross has caused extreme emotional distress for Mr. Ross. The loss of his savings caused massive disruption in Mr. Ross' financial planning and caused him to worry about the financial well-being of himself and his daughter. He has suffered, and continues to suffer, from severe anxiety, fear, weight gain, depression, and loss of sleep as a direct result.

50. Additionally, Mr. Ross' and his minor daughter's sensitive and confidential personal information have been compromised as a result of the SIM swaps. Mr. Ross stored color copies of their passports, drivers' licenses, and birth certificates in the online accounts which were taken over by the hackers as a result of the AT&T-facilitated SIM swap. Ten years of Mr. Ross' sensitive and confidential tax returns were also compromised. All of this information is now at extraordinarily high risk of being posted or bought and sold on the dark web by criminals and identity thieves, putting Mr. Ross and his minor child at ongoing risk of significant privacy violations, identity theft, and countless additional unknown harms for the rest of their lives.

### C. AT&T's Failure to Protect Mr. Ross' Account from Unauthorized Access Violates Federal Law

51. AT&T is the world's largest telecommunications company and provider of mobile telephone services. As a common carrier,7F[8] AT&T is governed by the Federal Communications Act of 1934, as amended ("FCA"),8F[9] and corresponding regulations passed by the FCC.9F[10]

52. Recognizing the sensitivity of data collected by mobile carriers, Congress, through the FCA, requires AT&T to protect Mr. Ross' sensitive personal information to which it has access as a result of its unique position as a telecommunications carrier.10F[11]

53. Section 222 of the FCA, which became part of the Act in 1996, requires AT&T to protect the privacy and security of information about its customers. Likewise, Section 201(b) of the Act requires AT&T's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.11F[12]

54. AT&T's most specific obligations to protect its customers concerns a specific type of information, called Customer Proprietary Information and Other Customer Information, and known by the acronym "CPNI."12F[13] Specifically, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."13F[14]

55. Carriers like AT&T are liable for failures to protect their customers unauthorized disclosures.14F[15] The FCC has also stated that "[t]o the extent that a

[8] 47 U.S. Code § 153(51).
[9] 47 U.S.C. § 151 *et seq.*
[10] 47 C.F.R. § 64.2001 *et seq.*
[11] 47 U.S.C. § 222.
[12] 47 U.S.C. § 201(b).
[13] 47 U.S.C. § 222(a).
[14] Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927 ¶ 1 (April 2, 2007) (hereafter, "2007 CPNI Order").
[15] 47 U.S.C. §§ 206, 207.

carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred."15F[16]

56. CPNI is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."16F[17]

57. As AT&T has admitted to customers, SIM swap attacks constitute a CPNI breach.

58. Mr. Ross' CPNI was breached by one or more AT&T employees, representatives and agents when they accessed his account and swapped his SIM card number without his authorization. When employees, representatives and agents accessed Mr. Ross' account, his CPNI was visible. On information and belief, this included, but was not limited to, information about the configuration, type, and use of his subscribed AT&T services, his personal information, his SIM card details, and his billing information. AT&T employees, representatives and agents then used this information to effectuate an unauthorized SIM swap.

59. This type of unauthorized use of Mr. Ross' CPNI is illegal under the FCA. The FCA forbids AT&T from "us[ing], disclos[ing], or permit[ting] access to" CPNI, except in limited circumstances.17F[18] This extends to the carrier's employees, representatives and agents.

---

[16] Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) (hereafter, "2013 CPNI Order").

[17] 47 U.S.C. § 222(h)(1).

[18] 47 U.S.C. § 222(c)(1).

60. AT&T may only use, disclose, or permit access Mr. Ross' CPNI: (1) as required by law; (2) with his approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[19] Beyond such use, "the Commission's rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI."[20]

61. AT&T failed to protect Mr. Ross from authorized use of his CPNI. AT&T permitted its employees, representatives and agents to use and/or disclose Mr. Ross' CPNI without obtaining Mr. Ross' knowing consent beforehand. AT&T employees,representatives and agents, acting within the scope of their employment and agency, likewise did not seek Mr. Ross' knowing consent before using, disclosing, and/or permitting access to his CPNI when they accessed his account and swapped his SIM card. Instead, AT&T employees, representatives and agents authorized a COAM SIM swap over the phone, in violation of AT&T's own internal policies. Because such conduct does not fit within the FCA's recognized legitimate uses, it constitutes a violation of the FCA.

62. Pursuant to the FCA, the FCC has developed comprehensive rules concerning AT&T's obligations under its duty to protect customers' CPNI.[21] This includes rules "designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI."[22] The FCC specifically recognizes that "[a]bsent carriers' adoption of adequate security safeguards, consumers' sensitive information… can be disclosed to third parties without consumers' knowledge or consent."[23] In a 2013 order,

---

[19] 47 U.S.C. § 222.
[20] 2007 CPNI Order ¶ 8 (emphasis added).
[21] *See* 47 CFR § 64.2001("The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222."). The FCC also regularly releases CPNI orders that promulgate rules implementing its express statutory obligations. *See* 2007 CPNI Order and 2013 CPNI Order.
[22] 2007 CPNI Order ¶ 9; *see also Id.* at ¶ 35; 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.
[23] *Id.*

the FCC "clarif[ied] existing law so that consumers will know that *their carriers must safeguard these kinds of information so long as the information is collected by or at the direction of the carrier and the carrier or its designee*[24] *has access to or control over the information*."[25]

63. Pursuant to these rules, AT&T must "implement a system by which the status of a customer's CPNI approval can be clearly established *prior to* the use of CPNI."[26] AT&T is also required to "design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established."[27] The FCC's rules also "require carriers to maintain records that track access to customer CPNI records."[28]

64. Upon information and belief, AT&T has failed to implement such a system. The fact that Mr. Ross' account was accessed, and his SIM card number was changed without his authorization, demonstrates AT&T's failures in this regard.

65. AT&T is also required to "train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place."[29]

66. Upon information and belief, AT&T has failed to properly train and supervise its personnel, contractors, representatives and agents, as reflected by an AT&T employee,representative and agent's involvement in Mr. Ross' breaches – and that employee, representative's and agent's ability to so easily effectuate a SIM swap in violation of AT&T's own internal policies.

---

[24] In the ruling, "designee" is defined as "an entity to which the carrier has transmitted, or directed the transmission of, CPNI or is the carrier's agent." *Id.* n. 1.
[25] *Id.* at ¶ 1 (emphasis added).
[26] 2007 CPNI Order ¶¶ 8-9 (emphasis added); *see also* 47 C.F.R. § 64.2009(a).
[27] *Id.* ¶ 9.
[28] *Id.*
[29] 47 C.F.R. § 64.2009(b) "Safeguards required for use of customer proprietary network information".

67. AT&T has also breached its duty to safeguard Mr. Ross' CPNI from data breaches, in violation of Section 222(a) and Section 201(b) of the FCA.

68. The FCC has "[made] clear that carriers' existing statutory obligations to protect their customers' CPNI include[s] a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."29F[30]

69. AT&T failed to take reasonable steps to protect Mr. Ross' CPNI, thereby allowing third-party hackers to access his CPNI.

70. The FCC also requires that carriers inform customers – and law enforcement – "whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization."30F[31] This requirement extends to *any* unauthorized disclosure.

71. In adopting this requirement, the FCC rejected the argument that it "need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure."31F[32]

72. Instead, the FCC found that "[i]f customers and law enforcement agencies are unaware of [unauthorized access], unauthorized releases of CPNI will have little impact on carriers' behavior, and thus provide little incentive for carriers to prevent further unauthorized releases. By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever 'next steps' are appropriate in light of the customer's particular situation."32F[33] The FCC

[30] 2007 CPNI Order ¶ 36 (citation omitted).
[31] 2007 CPNI Order at ¶ 26; *see also* 47 C.F.R § 64.2011(c).
[32] 2007 CPNI Order ¶ 30.
[33] *Id.*

specifically recognized that this notice could allow consumers to take precautions or protect themselves "to avoid stalking or domestic violence."33F[34]

73. AT&T failed in its duty to safeguard Mr. Ross' CPNI from breaches and, upon information and belief, has failed to properly inform him of such breaches when they occurred. Mr. Ross never received any documentation or communication alerting him that his CPNI had been breached, even though AT&T knew his CPNI had been breached as a result of the REACT criminal investigation, and knew or should have known that his CPNI had been breached as a result of multiple prior SIM swaps enacted by hackers using the same mobile phone and IMEI.

74. Under the FCA, AT&T is not just liable for its own violations of the Act, but also for violations that it "cause[s] or permit[s]."34F[35] By failing to secure Mr. Ross' account and protect his CPNI, AT&T caused and/or permitted Mr. Ross' CPNI to be accessed and used by its own employees, representatives and agents and by third-party hackers.

75. AT&T is also responsible for the acts, omissions, and/or failures of officers, agents, employees, or any other person acting for or employed by AT&T.

**D. Mr. Ross' Harm was Caused by Defendants' Negligence**

76. By failing to secure Mr. Ross' account—and protect the confidential and sensitive data contained therein—and to properly hire, train, and supervise their employees, representatives and agents, Defendants are responsible for the foreseeable harm Mr. Ross suffered as a result of Defendants' gross negligence.

77. Further, Defendants are responsible for their representatives' and agents' failure to obtain Mr. Ross' valid consent before accessing his account and

---

[34] *Id.* at n. 100.

[35] *See* 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]")

effectuating a SIM swap, as such actions were within the scope of their agency of employment with Defendants. On information and belief, Defendants' representatives and agents were tasked with and able to change customers' SIM card numbers at will – even when such changes violated AT&T company policy.

78. Additionally, Defendants representatives' and agents' breach of Mr. Ross' account and the subsequent SIM swap was foreseeable.

79. AT&T has known for more than a decade that third parties frequently attempt to access and take over mobile customers' accounts for fraudulent purposes.

80. In 2007, the FCC issued an order strengthening its CPNI rules in response to the growing practice of "pretexting."35F[36] Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communication records."36F[37] This 2007 Order put AT&T on notice that its customers' accounts were vulnerable targets of the third-parties seeking unauthorized access.

81. AT&T and its representatives and agents also knew, or should have known, about the risk SIM swap crimes presented to its customers. SIM swap crimes have been a widespread and growing problem for years. The U.S. Fair Trade Commission ("FTC") reported in 2016 that there were 1,038 reported SIM swap attacks *per month* in January 2013, which increased sharply to 2,658 per month by January 2016—2.5 times as many.37F[38] The FTC reported that SIM swaps represented 6.3% of all identity thefts reported to the agency in January

[36] 2007 CPNI Order.
[37] *Id.* at ¶ 1.
[38] Lori Cranor, FTC Chief Technologist, "Your mobile phone account could be hijacked by an identity thief," Federal Trade Commission (June 7, 2016), *available at* https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (hereafter, "2017 FTC Report").

2016, and that such thefts "involved all four of the major mobile carriers" – including AT&T.[39]

82. AT&T knew or should have known that it needed to take steps to protect its customers. The FTC's 2017 Report stated that "*mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking*[.]"[40] The FTC urged carriers like AT&T to "adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions."[41] The FTC also specifically warned carriers like AT&T of the risk that, due to text message password reset requests and two-factor authentication, SIM swapping put subscribers at risk of financial loss and privacy violations:

> Having a mobile phone account hijacked can waste hours of a victim's time and cause them to miss important calls and messages. However, this crime is particularly problematic due to the growing use of text messages to mobile phones as part of authentication schemes for financial services and other accounts. The security of two-factor authentication schemes that use phones as one of the factors relies on the assumption that someone who steals your password has not also stolen your phone number. *Thus, mobile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.*[42]

83. AT&T admitted it was aware of SIM swap crimes and the effect they could have on its customers in September 2017 when AT&T's Vice President of Security Platforms published an article on AT&T's "Cyber Aware" blog about SIM swaps.[43] In the article, AT&T acknowledged that subscribers with "valuable

---

[39] *Id.*
[40] *Id.* (emphasis added).
[41] *Id.*
[42] *Id.* (emphasis added).
[43] Brian Rexroad, "Secure Your Number to Reduce SIM Swap Scams," AT&T's Cyber Aware (Sep. 2017), *available at* https://about.att.com/pages/cyberaware/ni/blog/sim_swap.

accounts that are accessible online" are likely targets of SIM swaps. AT&T recommended that its customers set up passcodes that would provide "extra security." These passcodes failed to protect Mr. Ross.

84. AT&T therefore knew that its customers' accounts were at risk for *longer than a year* before Mr. Ross' account was breached.

85. AT&T's inadequate security procedures are particularly egregious in light of AT&T's repeated public statements about the importance of cyber security and its public representations about its expertise in this area. AT&T has an entire series on its public YouTube channel ("AT&T ThreatTraq") dedicated to discussing and analyzing emerging cybersecurity threats.[44] In its videos, AT&T describes itself as a "network that senses and mitigates cyber threats."[45]

86. AT&T recognizes the risks that arise when a mobile phone is compromised, stating, "Our phones are mini-computers, and with so much personal data on our phones today, it's also important to secure our mobile devices."45F[46] AT&T's advertisements also stress how central a role mobile phones play in its customer's lives, stating: "My phone is my life" and "My phone is everything." The same ad stresses how the inability to use a mobile phone makes people feel "completely untethered, flailing around."[47]

87. AT&T markets its ability to identify and neutralize emerging cyber threats for its customers. In one video, AT&T employees discuss "threat hunting" – which they describe as "an active threat analysis where you're actually thinking about your adversary."[48] They claim that it's "important" and "something [AT&T

---

[44] "AT&T Tech Channel," YouTube, *available at* https://www.youtube.com/user/ATTTechChannel.

[45] "AT&T – Protect Your Network with the Power of &," VIMEO, *available at* https://vimeo.com/172399153.

[46] AT&T, "Mobile Security," YOUTUBE (Feb. 12, 2019), *available* at https://www.youtube.com/watch?v=KSPHS89VnX0.

[47] "AT&T Mobile Movement Campaign – Ads," VIMEO, *available at* https://vimeo.com/224936108.

[48] AT&T Tech Channel, "The Huntin' and Phishin' Episode," YOUTUBE (Apr. 21, 2017), *available at* https://www.youtube.com/watch?v=3g9cPCiFosk.

has] been doing for a long time."[49] They advise that companies should think about "what would a hacker want to do, where would a hacker go to get my data, what are some of the points on my network that are most vulnerable, or where is the data flow that is potentially going to be a leakage" and state that "having threat hunting as part of a proactive continuous program, integrating with existing security measures, will help [you] stay ahead of the threats."[50] AT&T failed to heed this advice.

88. Not only did AT&T advise staying ahead of and addressing cyber threats, it also stressed that these practices could even help identify "insider threats"—*employees within the company or authorized representatives and agents.*

89. In an additional video focused on insider threats, AT&T representatives go on at length about the threat of company insiders selling corporate information *and access*, citing a survey showing that "30% [of respondents] had purposefully sent data outside of their organization at some point in time" and "14% of the people that were interviewed said they would actually sell their corporate log-ins to folks on the outside or sell that data for less than about $250 US."[51] They cited as a "significant concern" the "individuals that have privileged access, that have broad access inside an organization."[52] AT&T therefore knew or should have known that there was a significant risk that its own employees, representatives and agents would provide AT&T customer data—including customer account data—and that the risk was heightened when employees had too broad of access to corporate systems, yet failed to put sufficient systems and resources in place to mitigate that risk, despite its own advice to the contrary.

---

[49] *Id.*
[50] *Id.*
[51] AT&T ThreatTraq, "The Real Threat of Insider Threats," YouTube (May 5, 2017), *available at* https://www.youtube.com/watch?v=ZM5tuNiVsjs (emphasis added).
[52] *Id.*

90. AT&T has also recognized the danger presented to its customers when their email addresses are hacked, as Mr. Ross' was as a result of AT&T's failures. As one AT&T employee puts it: "I think most people do have something valuable [in their email accounts], which is access to all their other accounts, which you can get with a password reset."[53] They call this "something worth keeping safe."[54] They advised that a "strong, obviously, security awareness program within a company… is extremely important."[55]

91. In this online video series, AT&T makes specific mention of SIM swapping activity. In one video, AT&T's Vice President of Security Platforms (Brian Rexroad) and Principal of Technology Security (Matt Keyser) discuss the hack of a forum called OGusers.[56] In the segment, they discuss the hacking of social media users' account names and point to a news story that highlights—in distinct orange type—that OGusers is a forum popular among people "conducting SIM swapping attacks to seize control over victims' phone numbers."[57]

[53] *Id.*
[54] *Id. See also* "Account Hijacking Forum OGusers Hacked", KREBSONSECURITY (May 19, 2019) *at* https://krebsonsecurity.com/2019/05/account-hijacking-forum-ogusers-hacked/
[55] *Id.*
[56] AT&T ThreatTraq, "5/31/19 Account-hacking Forum OGusers Hacked," YOUTUBE (May 31 2019), *available at* https://www.youtube.com/watch?time_continue=234&v=cS4xV3cej3A.
[57] *Id.*; *see also* Freeman Indictment at ¶ 2 (Describing how "discussions—such as discussing the manner and means to [SIM swap] attacks generally, and networking among [SIM swap hackers]—typically took place on forums such as "OGusers.").


*Figure 2*

92. AT&T was therefore well aware of the significant risk that AT&T employees, representatives and agents and SIM swapping presented to its customers, and the need to mitigate such risks, but nonetheless failed to take adequate steps to protect Mr. Ross. Instead, it continued to make public statements giving rise to a reasonable expectation that AT&T could—and would—protect its customers, and at the same time invested millions of dollars into ZenKey to profit from the problem.

93. That Mr. Ross was at risk of account breaches at the hands of AT&T employees, representatives and agents is particularly foreseeable—and AT&T's failures are particularly stark—in light of AT&T's history of unauthorized employee, representative and agent access to customer accounts.

94. In 2015, AT&T faced an FCC enforcement action, and paid a $25 million civil penalty, for nearly identical failures to protect its customers' sensitive account data.[58] In that case, as AT&T admitted, employees, representatives and

[58] *In the Matter of AT&T Servs., Inc.*, 30 F.C.C. Rcd. 2808 (2015) at https://docs.fcc.gov/public/attachments/DA-15-399A1.pdf

agents at an AT&T call center breached 280,000 customers' accounts.[59] Specifically, AT&T employees, representatives and agents had improperly used login credentials to access customer accounts and access customer information that could be used to unlock the customers' devices.[60] The employees then sold the information they obtained from the breaches to a third party.[61]

95. The FCC concluded that AT&T's "failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act."[62]

96. The FCC stressed that the FCA is intended to "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information."[63] It stressed its expectation that "telecommunications carriers such as AT&T… take 'every reasonable precaution' to protect their customers' data[.]"[64]

97. As part of its penalty, AT&T entered into a stipulated Consent Decree with the FCC, in which AT&T agreed to develop and implement a compliance plan to ensure appropriate safeguards to protect consumers against similar breaches by improving its privacy and data security practices.[65]

98. This FCC enforcement action underscores AT&T's knowledge of the risk its employees presented to customers, the prevalence of employee breaches to customer data, the sensitive nature of customer CPNI, and its duties to protect and safeguard that data. Nonetheless, more than 3 years after stipulating to the Consent Decree, AT&T still failed to protect its customer from employee breaches of

[59] *Id.* at ¶ 1.
[60] *Id.* at ¶¶ 7, 11.
[61] *Id.* at ¶ 1.
[62] *Id.* at ¶ 2.
[63] *Id.*
[64] *Id.*
[65] *Id.* at ¶¶ 2, 17-18, 21.

customer CPNI and other account data, virtually identical to the breach at issue here, heightening the degree of its negligence. In January 2020, Princeton researchers released a study finding that top U.S. mobile carriers, including AT&T, do little to protect customers from SIM swap fraud.[66] The study stated "We examined the authentication procedures used by five prepaid wireless carriers when a customer attempted to change their SIM card. ***We found that all five carriers used insecure authentication challenges that could be easily subverted by attackers***. We also found that attackers generally only needed to target the most vulnerable authentication challenges, because the rest could be bypassed." The researchers pretended to be the true phone owner and said they forgot answers to security questions study stating, "Our key finding is that, at the time of our data collection, all 5 carriers used insecure authentication challenges that could easily be subverted by attackers." The study also found: (i) Callers only needed to successfully respond to one challenge in order to authenticate, even if they had failed numerous prior challenges. (ii) Four-fifths of SIM-swap fraud attempts were successful, and the researchers attempted 50 SIM swaps and successfully completed 39. (iii) AT&T, Verizon and T-Mobile failed the study. (iv) Some carriers even guided them to the correct answer or didn't ask for anything at all. The Princeton study was widely reported in the media and prompted Congress to get involved. In January 2020, Senator Ron Wyden and 5 other Senators and Congressmen published a letter to FCC Chairman Ajit Pai calling on him to take action to protect consumers against SIM swap fraud, with the Senator stating "SIM swap fraud may also endanger national security. For example, if a cybercriminal or foreign government uses a SIM swap to hack into the email account of a local public safety official, they could then leverage that access to issue emergency

---

[66] *"An Empirical Study of Wireless Carrier Authentication for SIM Swaps"* Kevin Lee, Ben Kaiser, Jonathan Mayer, Arvind Narayanan Dept of Computer Science and Center for Information Technology Policy, Princeton University, January 10, 2020 at https://www.issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf

alerts using the federal alert and warning system operated by the Federal Emergency Management Agency."[67] Senator Wyden also stated, "Consumers are at the mercy of wireless carriers when it comes to being protected against SIM swaps."[68]

99. According to a Wall Street Journal ("WSJ") article from November 2019, "He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers," investigators say they know of more than 3,000 SIM swap victims, accounting for at least $70 million in theft nationwide (the real numbers are likely much higher considering that many cases go unreported).[69] The WSJ article states, "the people who investigate these attacks consider them some of the most harmful they have ever seen." [69] Victims include high profile public officials, celebrities, and business executives like Jack Dorsey, the CEO of Twitter, whose 2019 SIM swap hack was profiled in the Forbes article "Why Twitter Blames AT&T For The Hack Of Its CEO Jack Dorsey Account, Sending Shocking Racist Tweets," and quotes Jeb Su, a Principal Analyst at Atherton Research as saying "*AT&T's poor security policy made this malicious [SIM swap] hack possible.*" [70] The same hacker who executed Jack Dorsey's SIM swap also successfully hacked the District Attorney prosecuting the hacker who AT&T gave control to Mr. Ross' phone service.[71]

100. For many years AT&T has been fully aware of well-established solutions to deter and prevent unauthorized SIM swaps and resulting thefts, which it could easily have implemented well *before* Mr. Ross' phone was SIM swapped, but failed and refused to implement:

---

[67] https://docs.fcc.gov/public/attachments/DOC-362599A1.pdf
[68] https://twitter.com/ronwyden/status/1215757690875600896
[69] https://www.wsj.com/articles/he-thought-his-phone-was-secure-then-he-lost-24-million-to-hackers-11573221600.
[70] https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-for-ceo-jack-dorsey-account-hack-sending-shocking-racist-tweets/.
[71] *"Authorities Arrest Alleged Member of Group That Hacked Jack Dorsey*", Vice by Joseph Cox, November 23, 2019 at https://www.vice.com/en_us/article/gyzawx/authorities-arrest-suspected-jack-dorsey-hacker.

a. Location detection. At the exact moment of the SIM swap request, AT&T knew the hacker's phone was in New York City (as detailed in the location data AT&T provided to REACT)[7] and that Mr. Ross' phone was simultaneously in San Francisco, as AT&T tracks customers' location and even sells their location data (following an investigation into this practice, the FCC proposed $57 million in fines against AT&T).[72] AT&T knew that Mr. Ross and his phone could not simultaneously be in both San Francisco and New York City, and could have easily recognized the SIM swap request as a fraud attempt, denied it, and alerted Mr. Ross. AT&T was actually profiting off customers' location data at the same time as it did nothing to use the same location data to prevent the unauthorized SIM swap.

b. Text message. AT&T could have simply sent Mr. Ross a text message asking him to confirm whether he requested the SIM swap. He would have replied "no" and AT&T would have then denied the hacker's SIM swap request and could have reported the fraud attempt to Mr. Ross. Banks regularly text customers in this way to confirm even small, low-risk transactions to prevent fraud, as in the text Mr. Ross received from Bank of America confirming $1 transactions in Figure 3.

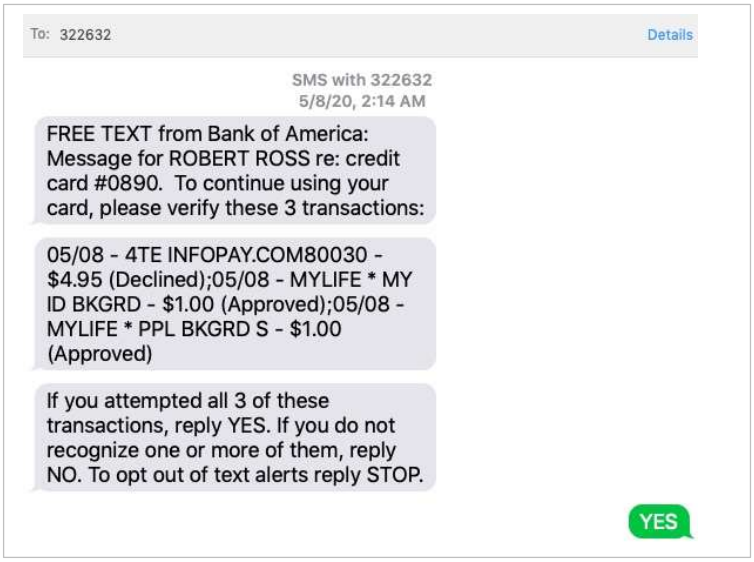



Figure 3

[72] FCC Proposes Over $200 Million in Fines Against Four Largest Wireless Carriers For Apparently Failing to Adequately Protect Consumer Location Data February 28, 2020 at https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf

AT&T regularly sends text messages to its customers for marketing purposes, and asks customers to reply if they want to stop receiving such texts, as in the message AT&T sent to Mr. Ross in Figure 4.

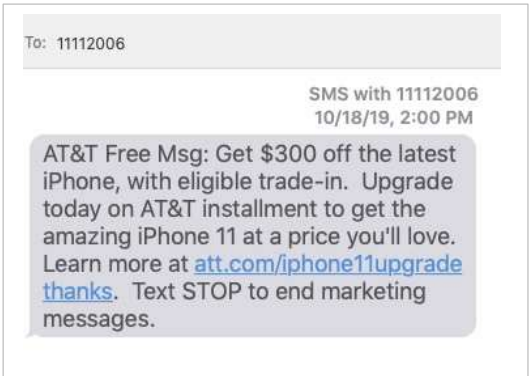



Figure 4

AT&T obviously has the ability to send such simple text messages to its customers requesting a reply. It is hard to fathom that AT&T used its own texting service to offer Mr. Ross an iPhone promotion, but refused to send him a simple text to prevent a high-risk SIM swap, and instead devastated his life.

c. IMEI detection. AT&T detects when the same phone has been used in prior unauthorized SIM swaps, and their records (as provided to REACT) show that, prior to the unauthorized SIM swap AT&T facilitated against Mr. Ross, the same device as identified by its IMEI was used in 11 previous unauthorized SIM swaps.[7] AT&T could simply have denied the ability for the phone that was used in previous unauthorized SIM swaps to be used in subsequent SIM swaps, including Mr. Ross', and also could have alerted Mr. Ross to the fraud attempt.

d. Voice biometrics. Often branded as "Voice ID," voice biometrics is a well-established and cost-effective technology that has been implemented by leading financial institutions (e.g., Chase, Wells Fargo and Schwab) to prevent fraud by verifying customers' identities by comparing a caller's voice to a customer (or fraudster) voiceprint stored on file.[73] AT&T developed its

[73] Chase at https://www.chase.com/personal/voice-biometrics, Wells Fargo at https://www.wellsfargo.com/privacy-security/voice-verification, and Schwab at https://www.schwab.com/voice-id.

own voice biometrics as part of its "AT&T Watson" technology platform, and was granted multiple patents.[74] AT&T sold the Watson platform and related patents to Interactions Corporation ("Interactions") in 2014 in exchange for an equity stake.[75] At least a dozen of AT&T Watson's core speech technologists and scientists transferred to Interactions at the time of the transaction.[76] While AT&T's technology and patents were also transferred to Interactions, the AT&T inventors of these voice biometrics patents remained at AT&T.[77] Interactions continues to promote its voice biometrics solution as "Secure and Convenient Authentication."[78] AT&T did not implement the "Watson" solution it developed in-house to prevent SIM swap fraud, and has also not implemented the solutions offered by industry leaders such as Nuance Communications, whereas non-US carriers, such as Deutsche Telekom, the largest telecommunications company in Europe, do.[79] Ironically, while AT&T refuses to implement such a voice biometrics solution, it continues to publicly promote the solution to its large corporate customers who have their own call centers (e.g., banks, insurance companies), and published a research report entitled "4 emerging technologies that could transform your contact center," which provides in relevant part as follows:

> Even as companies take steps to guard their IT environments against a growing barrage of cyberthreats,

---

[74] "Voice over IP based biometric authentication" https://patents.google.com/patent/US7254383; https://patents.google.com/patent/US7995995; https://patents.google.com/patent/US861521; https://patents.google.com/patent/US20140075530; "Centralized biometric authentication" https://patents.google.com/patent/US7324946B2

[75] *AT&T and Interactions Agree to Strategic Transaction in Speech and Multi-Modal Technology Arena* November 5, 2014. https://about.att.com/story/att_and_interactions_agree_to_strategic_transaction_in_speech_and_multi_modal_technology_arena.html

[76] LinkedIn > Search on Current Company: Interactions, Past Company: AT&T

[77] Brian Novack, AT&T (https://www.linkedin.com/in/brian-novack-10478b1); Daniel Madsen, AT&T (https://www.linkedin.com/in/daniel-madsen-05255846); Timothy Thompson, AT&T (https://www.linkedin.com/in/timothy-thompson-60ba391).

[78] https://www.interactions.com/products/voice-biometrics/

[79] *Deutsche Telekom turns to biometrics for authentication and fraud detection* https://telecoms.com/491915/dt-turns-to-biometrics-for-authentication-and-fraud-detection/

> many are neglecting another vulnerable area: their contact centers.
>
> Social engineering calls to contact centers — in which fraudsters pose as customers and try to trick agents into revealing confidential customer information — are on the rise, according to industry experts, particularly at financial institutions, insurance companies and other businesses that store sensitive data.
>
> Voice biometrics can help your agents know exactly with whom they're talking when they answer a customer call. This technology can recognize voice characteristics passively and verify callers in real time, whether they need to speak to one of your representatives or are using your interactive voice response system.
>
> "By comparing your callers' voiceprints against a database of known fraudster voiceprints, voice biometrics programs can help you identify and track potential thieves before they steal your data."[80]

e. Data sharing. Mobile phone carriers in other countries have implemented a "data sharing" solution to prevent theft once an unauthorized SIM swap has occurred. In essence, the carriers allow financial institutions real-time access to their SIM swap data so that the institution can block a requested currency transfer if there has been a SIM swap within a specified time frame (e.g., within 48 hours of the transfer request), which together is a very strong indicator of fraud. The data sharing solution is widely known and used in the industry. Wired magazine published an article entitled "The SIM Swap Fix That the US isn't Using," which states in relevant part that "While foreign phone carriers are sharing

[80] "*4 Emerging Technologies That Could Transform Your Contact Center" Mike Rajich, AT&T Director of Contact Center and Enterprise Routing Product Management, AT&T* https://www.business.att.com/learn/research-reports/4-emerging-technologies-that-could-transform-your-contact-center.html

data to stop SIM swap fraud, US carriers are dragging feet."[81] Wired describes that even carriers in developing countries such as Mozambique implemented the solution within a few months of understanding the extent of the problem, and that the Head of IT, Cyber Security & Core Data Networks at Vodacom reported that "[the solution] reduced their SIM swap fraud to nearly zero overnight".[82] Such data sharing to combat fraud resulting from unauthorized SIM swaps is widely adopted and has given rise to several multimillion dollar third party aggregators, including Prove.com (formerly Payfone, Inc.) and Telesign Corporation, who license SIM swap data from carriers and sell it as a risk management offering to banks. Figure 5 shows hoq all four major carriers in the United Kingdom ("UK"), including British Telecom, Vodafone, O2 and Three, provide their SIM swap data to Prove.com, which in turn sells services to banks to do real-time SIM swap checks to prevent fraud at the time of their customers' high-risk transactions.[83]

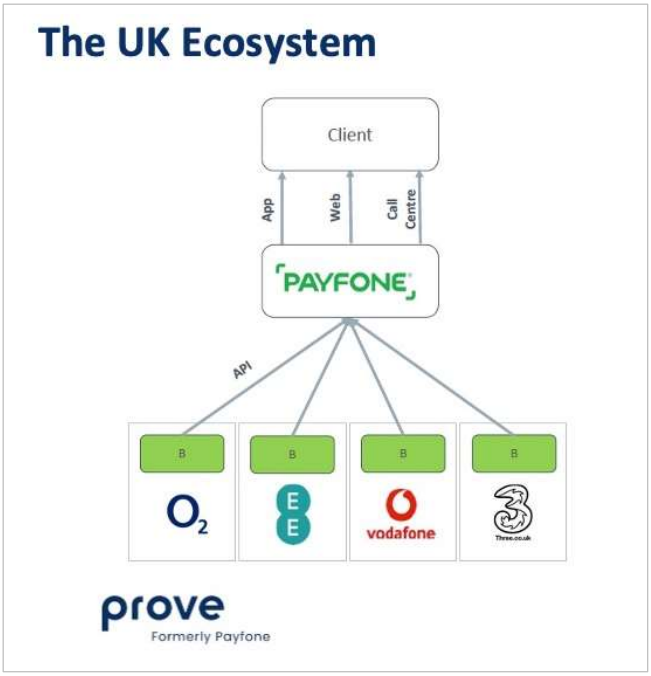



Figure 5

[81] *The SIM Swap Fix That the US Isn't Using, Wired*, Andy Greenberg, April 26, 2019 https://www.wired.com/story/sim-swap-fix-carriers-banks/.
[82] Id.
[83] https://info.prove.com/psd2-sca-uk-mobile-authentication

101. On information and belief, AT&T failed and refused to implement location, text, IMEI and voice biometrics solutions, because it has made the cynical decision that corporate profits are more important than customer security. The various security measures which AT&T could have implemented, but deliberately chose not to, would have increased "customer friction." As noted by Forbes magazine, in the age of Amazon and Uber, "[t]he goal is to eliminate friction – to make things easier for the customer."[84] According to Augie Ray, the renowned Gartner Customer Experience analyst, "[b]rands are trying a lot of things to reduce customer friction points."[85] In addition, "[c]onsidering how customer loyalty is far from abundant these days, there are many ways to lose a customer, but the biggest turn-off for today's consumers is an experience in which friction isn't kept to a minimum." *Id*. "[T]here's a clear benefit to reducing customer friction points: it improves the bottom line." Id. In short, AT&T made the conscious decision that unauthorized SIM swaps affected such a small percentage of its 150 million customers that the benefits of reducing such fraud was outweighed by the cost of losing customers due to increased customer friction.

102. At the same time that AT&T was consciously not implementing solutions to the SIM swap problem, it was investing in a for-profit venture called ZenKey which markets an app which seeks to prevent theft *after* an illegal SIM swap has occurred. ZenKey is a joint venture between AT&T, Verizon and T Mobile and was originally made public on September 12, 2018 as "Project Verify", six weeks before the unauthorized SIM swap against Mr. Ross.[86] ZenKey is marketed to consumers as a two-factor authentication app which protects them from fraud, and marketed to financial institutions as an identity solution that can "

[84] https://www.forbes.com/sites/shephyken/2019/06/09/are-you-providing-a-frictionless-customer-experience/#538162864b8c

[85] https://thenextweb.com/contributors/2018/07/19/reducing-customer-friction-customer-loyalty/

[86] *U.S. Mobile Giants Want to be Your Online Identity* at https://krebsonsecurity.com/tag/project-verify/

increase conversions and improve customer satisfaction."[87] ZenKey seeks to charge fees to financial institutions in exchange for doing real-time checks against carrier databases to verify when a SIM swap (authorized or not) was last done,[88] and its Portal Agreement Terms of Service provides that "Certain services accessed or available through the [ZenKey] Portal, especially services for which You [e.g. a bank] are asked to subscribe or pay money, may have their own terms and conditions, including but not limited to the Service Agreement."[89] ZenKey promotes its service with the clear representation that its purpose is to combat SIM swap fraud: "With ZenKey, fraudsters can no longer access your users' accounts based on stolen credentials and a simple SIM Swap" [88] and "SIM swap fraud is on the rise and has cost businesses hundreds of millions of dollars…ZenKey offers a suite of APIs and event alerts (Trust Services) for Service Providers to receive on-demand fraud signals and automatic indicators."[90] On information and belief, while AT&T and its competitors collectively invested $200 million dollars into ZenKey, the venture has failed in the marketplace, and has not been adopted by financial institutions.

**F. Defendants Are Liable for the Acts of Their Employees, Representatives and Agents**

103. Defendants are liable for the acts of their employees, representatives and agents who facilitated the unauthorized access to, and resulting theft from, Mr. Ross.

104. Defendants failed to put in place adequate systems and procedures to prevent the unauthorized employee, representative and agent access to Mr. Ross' account and related data. Defendants failed to properly hire and supervise their employees, representatives and agents, allowing them to access Mr. Ross' sensitive

[87] https://myzenkey.com/business-benefits
[88] ZenKey website at https://myzenkey.com/trust-services/
[89] https://portal.myzenkey.com/terms
[90] https://myzenkey.com/business-benefits/

and confidential account data without his authorization and provide that data to third parties.

105. In the context of AT&T's enterprise as a telecommunications carrier, an employee, representative and agent accessing a customer's account information and effectuating a SIM swap—even without authorization—is not so unusual or startling that it would be unfair to include the loss resulting from such unauthorized access among other costs of AT&T's business – particularly in light of AT&T's awareness of the risk of SIM swaps to its customers.

106. Further, imposing significant liability on AT&T and its agents may prevent recurrence of SIM swap behavior because it creates a strong incentive for vigilance and proper safeguarding of customers' data by AT&T—which, in the case of its customers, is the sole party in the position to guard substantially against this activity, as it is the custodian and guardian of this data.

107. As a customer of AT&T, Mr. Ross is entitled to rely upon the presumption that AT&T and the employees, representative and agents entrusted with the performance of AT&T's business have faithfully and honestly discharged the duty owed to him by AT&T, and that they would not gain unauthorized access to his account.

108. The reasonableness of Mr. Ross' expectations that AT&T would safeguard his data is confirmed by the fact that the federal agency responsible for overseeing AT&T's duties to its customers, the FCC, has stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."65F[91]

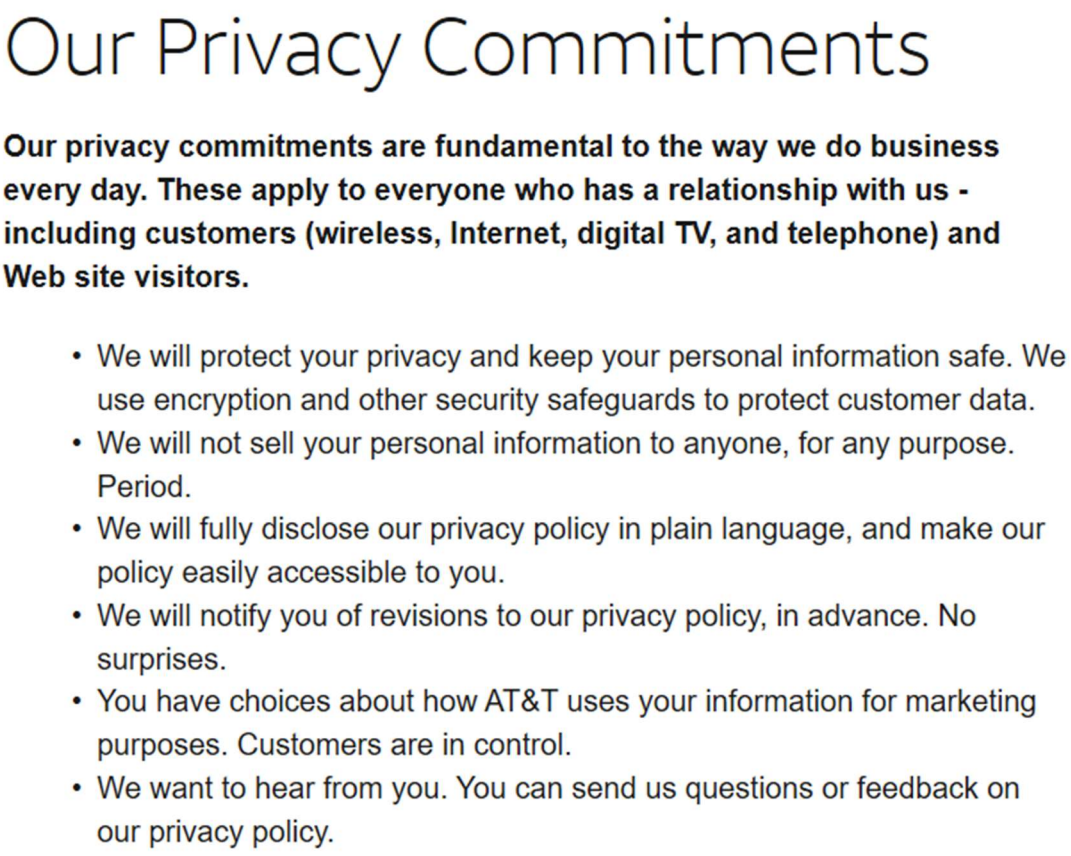
**F. AT&T's Misrepresentations and Omissions.**

109. AT&T's Privacy Policy, and the "Privacy Commitments" included therein, falsely represents and fails to disclose material information about its data security practices.

[91] 2007 CPNI Order ¶ 64.

110. In its Privacy Policy, AT&T promised to protect Mr. Ross' privacy and personal information, including by using "security safeguards." AT&T further pledges that it will not sell customer data.

These representations created an expectation that Mr. Ross' AT&T account and associated data would be safe and secure, that employees, representatives and agents would not access his account without authorization, that his data would be protected from unauthorized disclosure, and that he could control how and when his data was accessed. Figure 6, immediately below, is an excerpt from AT&T's Privacy Policy.



# Our Privacy Commitments

**Our privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with us - including customers (wireless, Internet, digital TV, and telephone) and Web site visitors.**

- We will protect your privacy and keep your personal information safe. We use encryption and other security safeguards to protect customer data.
- We will not sell your personal information to anyone, for any purpose. Period.
- We will fully disclose our privacy policy in plain language, and make our policy easily accessible to you.
- We will notify you of revisions to our privacy policy, in advance. No surprises.
- You have choices about how AT&T uses your information for marketing purposes. Customers are in control.
- We want to hear from you. You can send us questions or feedback on our privacy policy.

*Figure 6*66F[92]

[92] "Privacy Policy," AT&T, attached hereto as Exhibit C.

111. AT&T's representation that it "uses encryption and other security safeguards to protect customer data" is false and extremely misleading.

112. As alleged fully above, AT&T allowed its employees, representatives and agents to access Mr. Ross' account, and the CPNI and other sensitive data contained therein, without his authorization. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation.

113. Upon information and belief, AT&T's security safeguards were inadequate, including its system which—upon information and belief—allowed an individual employee, representative and agent to conduct SIM swaps without adequate technical safeguards and oversight, even when that employee, representative and agent authorizes a COAM SIM swap over the phone in violation of company policy.

114. "Having one employee who can conduct these SIM swaps without any kind of oversight seems to be the real problem," says Lieutenant John Rose, a member of the California-based Regional Enforcement Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement partnership specializing in cybercrime.67F[93] "And it seems like [the carriers] could really put a stop to it if there were more checks and balances to prevent that. It's still very, very easy to SIM swap, and something has to be done because it's just too simple. Someone needs to light a fire under some folks to get these protections put in place."

115. AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee, representative and agent access to and take over of Mr. Ross' account and related data. In connection with subsequent criminal investigations into Mr. Ross' SIM swap, AT&T informed law enforcement that it had the capacity to see how many different SIM cards had been associated

[93] Busting SIM Swappers and SIM Swap Myths," KREBSONSECURITY (Nov. 18, 2018), *available at* https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths.

with the same single mobile phone's IMEI.68F[94] In other words, AT&T could see when one mobile phone had multiple SIM cards associated with it in a short amount of time.69F[95]

116. AT&T also informed law enforcement that the hacker involved in Mr. Ross' SIM swap had requested that *eleven different phone numbers* be moved onto his phone (identified by its IMEI number) in the twenty-one days before Mr. Ross' swap.70F[96] The hacker sometimes moved three different AT&T numbers onto the same phone *in a single day*.71F[97] AT&T certainly had the capability to see this behavior, and could and should have flagged it as suspicious. If AT&T had proper security safeguards in place, it would have recognized this behavior, flagged it as suspicious, and prevented any further SIM swaps onto that phone – thereby protecting Mr. Ross.

117. Additionally, as alleged fully above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Ross' data was accessed and provided to third parties. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation. AT&T easily detected that the same phone was used in eleven prior unauthorized SIM swaps *before* the unauthorized SIM swap on Mr. Ross' phone, and gave this information to the REACT cybercrime task force.[7] However, AT&T did nothing to stop the hacker from using the same phone for multiple unauthorized SIM swaps, and had no voice biometric system or other solution in place to prevent the unauthorized SIM swaps.

118. AT&T's representation that it "will protect [customers'] privacy and keep [their] personal information safe" is false and misleading.

---

[94] Ex. B. at pp. 8, 22.
[95] *Id.*
[96] *Id.*
[97] *Id.* at 22.

119. As alleged fully above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Ross' account and the data therein were accessed and used without his authorization or consent and disclosed to third parties. Mr. Ross' privacy and personal information was not safe, as demonstrated by the breach of his AT&T account. AT&T's statement that it would protect customers' privacy and keep their personal information safe is therefore a material misrepresentation.

120. AT&T also makes numerous false or misleading representations concerning its treatment of customers' data that qualifies as CPNI under the FCA.

121. AT&T explicitly and falsely represents in its Privacy Policy that it does not "sell, trade or share" their CPNI:

> We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies* or our authorized agents, unless required by law (example: a court order).72F[98]

122. As alleged fully above, AT&T and its employees, representatives and agents provided access to Mr. Ross' CPNI to third-party hackers. This use was not required by law and was instead *prohibited* by law.

123. AT&T also states that it only uses CPNI "internally" and its *only* disclosed use of CPNI is "among the AT&T companies and our agents in order to offer you new or enhanced services."73F[99]

124. Defendants' employees', representatives' and agents' use of Mr. Ross' account and related data as described herein was not for "internal" AT&T purposes, nor was it used to market AT&T services. AT&T's statements regarding the use of

---

[98] "Customer Proprietary Network Information (CPNI)," AT&T, Ex. C at 31-32. The "AT&T family of companies" is defined as "those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services." *Id.*

[99] *Id.*

customer CPNI are therefore material misrepresentations. Its failure to disclose this is a material omission.

125. AT&T also falsely represents that it "uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI."

126. As alleged fully above, AT&T and its agents failed to safeguard Mr. Ross' CPNI. Instead, it stored customer CPNI in such a way that unauthorized access was easily obtained by employees and third parties. AT&T's statements regarding the technology and security features it uses to safeguard customer CPNI are therefore material misrepresentations.

127. AT&T was obligated to disclose the weaknesses and failures of its account and data security practices, as AT&T had exclusive knowledge of material facts not known or knowable to its customers, AT&T actively concealed these material facts from Mr. Ross, and such disclosures were necessary to materially qualify its representations that it took measures to protect consumer data and to materially qualify its partial disclosures concerning its use of customers' CPNI. Further, AT&T was obligated to disclose its practices under the FCA.

128. A reasonable person would be deceived and misled by AT&T's misrepresentations, which clearly indicated that AT&T would safeguard its customers' personal information and CPNI.

129. AT&T intentionally misled Mr. Ross regarding its data security practices in order to maintain his business, make money from his account, and evade prosecution for its unlawful acts. Furthermore, AT&T has invested millions into ZenKey to profit from the SIM swap problem, thereby incentivizing itself (and its 2 primary competitors) to not timely solve the problem to protect its customers, which other carriers have effectively solved.

130. AT&T's representations that it protected customers' personal information, when in fact it did not, were false, deceptive, and misleading and therefore a violation of the FCA.

## VI. CLAIMS FOR RELIEF

### COUNT I
### Violations of The Federal Communications Act, 47 U.S.C. § 201 *et seq.*

131. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

132. Defendants have violated 47 U.S.C. § 222(a) by failing to protect the confidentiality of Mr. Ross' CPNI, as detailed herein.

133. Defendants have violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting access to Mr. Ross' CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein. Defendants also caused and/or permitted third parties to use, disclose, and/or permit access to Mr. Ross' CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein.

134. As fully alleged above, Mr. Ross has suffered injury to his person, property, health, and reputation as a consequence of Defendants' violations of the FCA. Additionally, Mr. Ross has suffered emotional damages, including severe anxiety and depression, mental anguish, and suffering as a result of Defendants' acts and practices. These emotional damages have led directly to physical issues; for example, Mr. Ross began stress-eating which resulted in Mr. Ross gaining approximately 40 pounds in only a few months following the Defendants-facilitated thefts.

135. Mr. Ross seeks the full amount of damages sustained as a consequence of Defendants' violations of the FCA, together with reasonable attorneys' fees, to be fixed by the Court and taxed and collected as part of the costs of the case. Mr. Ross also moves for a writ of injunction or other proper process, mandatory or otherwise, to restrain Defendants and their officers, agents, or

representatives from further disobedience of the 2007 and 2013 CPNI Orders, or to compel their obedience to the same.

**COUNT II**
**Violations of The California Unfair Competition Law ("UCL") under the Unlawful, Unfair and Fraudulent Prongs, California Business & Professional Code § 17200 *et seq*.**

136. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

137. California's Unfair Competition Law (UCL) prohibits any "unlawful, unfair or fraudulent business act or practice." Defendants' business acts and practices complained of herein were unlawful, unfair, and fraudulent.

138. AT&T made material misrepresentations and omissions concerning its safeguarding of Mr. Ross' CPNI. As alleged fully above, a reasonable person would attach importance to the privacy of his sensitive account data in determining whether to contract with a mobile phone provider.

139. Defendants had a duty to disclose the nature of their inadequate security practices and failures in hiring, training, and supervising staff. Defendants had exclusive knowledge of material facts not known or knowable to AT&T customers and Defendants actively concealed these material facts from customers.

140. Further, additional disclosures were necessary to materially qualify AT&T's representations that it did not sell consumer data and took measures to protect that data, and its partial disclosures concerning its use of customers' CPNI. AT&T was obligated to disclose its practices, as required by the FCA. The magnitude of the harm suffered by Mr. Ross underscores the materiality of AT&T's omissions.

141. A reasonable person, such as Mr. Ross, would be deceived and misled by AT&T's misrepresentations, which indicated that Defendants would safeguard its customers' personal and proprietary information.

142. AT&T intentionally misled its customers regarding its data protection practices in order to attract customers and evade prosecution for its unlawful acts.

143. Defendants' actions detailed herein constitute an unlawful business act or practice. As alleged herein, Defendants' conduct is a violation of the California constitutional right to privacy and the FCA.

144. Defendants' actions detailed herein constitute an unfair business act or practice.

145. Defendants' conduct lacks reasonable and legitimate justification in that Mr. Ross has been misled as to the nature and integrity of AT&T's goods and services and has suffered injury as a result.

146. The gravity of the harm caused by Defendants' practices far outweigh the utility of their conduct. Defendants' practices were contrary to the letter and spirit of the FCA and its corresponding regulations, which require mobile carriers to disclose customers' CPNI only upon proper notice, consent, and authorization, and aims to vest carrier customers with control over their data. Due to the surreptitious nature of Defendants' actions, Mr. Ross could not have reasonably avoided the harms incurred as a result.

147. As the FCA establishes, it is against public policy to allow carrier employees or other third parties to access, use, or disclose telecommunications customers' sensitive account information. The effects of Defendants' conduct are comparable to or the same as a violation of the FCA.

148. Defendants' actions detailed herein constitute a fraudulent business act or practice.

149. As established herein, Mr. Ross has suffered injury in fact and economic harm as a result of AT&T's unfair competition. Additionally, had Defendants disclosed the true nature and extent of their data security and protection practices—and the flaws inherent in their systems—and their

unwillingness to properly protect its customers, Mr. Ross would not have subscribed to or paid as much money for AT&T's mobile services.

150. Mr. Ross seeks injunctive and declaratory relief for Defendants' violations of the UCL. Mr. Ross seeks public injunctive relief against Defendants' unfair and unlawful practices in order to protect the public and restore to the parties in interest money or property taken as a result of Defendants' unfair competition. Mr. Ross seeks a mandatory cessation of Defendants' practices, and proper safeguarding of AT&T account data.

**COUNT III**
**Violations of the California Constitutional Right to Privacy**

151. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

152. The California Constitution declares that, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. Art. I, § 1.

153. Mr. Ross has a reasonable expectation of privacy in his mobile device and his AT&T account information.

154. Defendants intentionally intruded on and into Mr. Ross' solitude, seclusion, or private affairs by allowing its employees and third parties to improperly access Mr. Ross' confidential AT&T account information without proper consent or authority.

155. The reasonableness of Mr. Ross' expectations of privacy is supported by AT&T and its agents' unique position to safeguard his account data, including the sensitive and confidential information contained therein, and protect Mr. Ross from SIM swap attacks.

156. AT&T and its agents' intrusions into Mr. Ross' privacy are highly offensive to a reasonable person. This is evidenced by federal legislation enacted by Congress and rules promulgated and enforcement actions undertaken by the

FCC aimed at protecting AT&T customers' sensitive account data from unauthorized use or access.

157. The offensiveness of Defendants' conduct is heightened by AT&T's material misrepresentations to Mr. Ross concerning the safety and security of his account.

158. Mr. Ross suffered great personal and financial harm by the intrusion into his private affairs, as detailed throughout this Complaint.

159. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Mr. Ross. But for Defendants' agents' and employees' unauthorized access to Mr. Ross' account and AT&T's failure to protect Mr. Ross from such harm through adequate security and oversight systems and procedures, Mr. Ross would not have had his personal privacy repeatedly violated and would not have been a victim of SIM swap theft resulting in his loss of $1,000,000 in cash and the breach of sensitive personal information

160. As a result of Defendants' actions, Mr. Ross seeks nominal and punitive damages in an amount to be determined at trial. Mr. Ross seeks punitive damages because Defendants' actions were malicious, oppressive, and willful. Defendants knew or should have known about the risks faced by Mr. Ross, and the grave consequences of such risks. Nonetheless, Defendants utterly failed to protect Mr. Ross, and instead, AT&T has invested millions of dollars into a scheme to profit from SIM swaps through ZenKey. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

**COUNT IV**
**Negligence**

161. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

162. Defendants owed a duty to Mr. Ross—arising from the sensitivity of his AT&T account information and the foreseeability of harm to Mr. Ross should

Defendants fail to safeguard and protect such data—to exercise reasonable care in safeguarding his sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing AT&T's and its agents', partners', and independent contractors' systems, protocols, and practices to ensure that Mr. Ross' information was adequately secured from unauthorized access.

163. Federal law and regulations, as well as AT&T's privacy policy, acknowledge Defendants' duty to adequately protect Mr. Ross' confidential account information.

164. Defendants owed a duty to Mr. Ross to protect his sensitive account data from unauthorized use, access, or disclosure. This included a duty to ensure that his CPNI was used, accessed, or disclosed only with proper consent.

165. Defendants owed a duty to Mr. Ross to implement a system to safeguard against and detect unauthorized access to Mr. Ross' AT&T data in a timely manner.

166. Defendants owed a duty to Mr. Ross to disclose the material fact that their data security practices were inadequate to safeguard Mr. Ross' AT&T account data from unauthorized access by its own employees and others.

167. AT&T had a special relationship with Mr. Ross due to its status as his telecommunications carrier, which provided an independent duty of care. AT&T had the unique ability to protect its systems and the data it stored thereon from unauthorized access.

168. Mr. Ross' willingness to contract with AT&T, and thereby entrust AT&T with his confidential and sensitive account data, was predicated on the understanding that AT&T and its agents would undertake adequate security and consent precautions.

169. Defendants breached their duties by, *inter alia*: (a) failing to implement and maintain adequate security practices to safeguard Mr. Ross' AT&T account and data—including his CPNI—from unauthorized access, as detailed

herein; (b) failing to detect unauthorized accesses in a timely manner; (c) failing to disclose that their data security practices were inadequate to safeguard Mr. Ross' data; (d) failing to supervise their agents and employees and prevent them from accessing and utilizing Mr. Ross' AT&T account and data without authorization; and (e) failing to provide adequate and timely notice of unauthorized access.

170. Defendants were also negligent in their authorization of Mr. Ross' SIM card swap. Defendants knew or should have known that at least ten different AT&T numbers had been moved to the same mobile phone (identified by its IMEI) in the weeks leading up to Mr. Ross' SIM swap. Defendants knew or should have known that this was highly suspicious. Nevertheless, Defendants effectuated the transfer of Mr. Ross' AT&T account to this same mobile phone. Defendants had the technical capacity to track this behavior—as reflected in its willingness to do so quickly for law enforcement—but nonetheless failed to utilize it for the benefit and protection of Mr. Ross.

171. But for Defendants' breaches of their duties, Mr. Ross' data would not have been accessed by unauthorized individuals.

172. Mr. Ross was a foreseeable victim of Defendants' inadequate data security practices and consent mechanisms. As alleged fully above, AT&T and its agents knew or should have known that SIM swaps presented a serious threat to its customers, including Mr. Ross, before Mr. Ross' account was breached for the first time. Defendants also knew or should have known that improper procedures and systems to safeguard customer data could allow their agents and employees to authorize customers' accounts and data, as occurred in the 2015 FCC enforcement action.

173. Defendants knew or should have known that unauthorized access would cause damage to Mr. Ross. AT&T admitted that unauthorized account access presents a significant threat to its customers, and it became aware during its

2015 FCC enforcement action of the harms caused by unauthorized account access.

174. Defendants' negligent conduct provided a means for unauthorized individuals to access Mr. Ross' AT&T account data, take over control of his mobile phone, and use such access to hack into numerous online accounts in order to rob Mr. Ross and steal his personal information.

175. As a result of Defendants' failure to prevent unauthorized accesses, Mr. Ross suffered grave injury, as alleged fully above, including severe emotional distress. This emotional distress arose out of Defendants' breach of their legal duties. The damages Mr. Ross suffered were a proximate, reasonably foreseeable result of Defendants' breaches of their duties.

176. Therefore, Mr. Ross is entitled to damages in an amount to be proven at trial.

177. The injury and harm suffered by Mr. Ross was the reasonably foreseeable result of AT&T's failure to exercise reasonable care in safeguarding and protecting Mr. Ross's Personal Information, including his CPI and CPNI. AT&T's misconduct as alleged herein is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Ross and despicable conduct that has subjected Mr. Ross to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Ross is entitled to punitive damages against AT&T under Civil Code § 3294(a). Mr. Ross further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

**COUNT V**
**Negligent Supervision and Entrustment**

178. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

179. AT&T conducts its business activities through employees or other agents, including One Touch Direct and One Touch Direct-SA.

180. Defendants are liable for harm resulting from their agents and employees because they was reckless or negligent in employing and/or entrusting agents and employees in work involving the risk of harm to others, including Mr. Ross.

181. On information and belief, Defendants knew or had reason to believe that their agents and employees were unfit and failed to exercise reasonable care in properly investigating and overseeing them. AT&T was negligent in supervising its agents and in entrusting them with what it knew to be highly sensitive confidential information. One Touch Direct and One Touch Direct-SA were negligent in supervising their agents and employees and in entrusting them with what they knew to be highly sensitive confidential information. Defendants knew or had reason to know that their agents and employees were likely to harm others in view of the work AT&T entrusted to them. Specifically, AT&T entrusted its agents and employees with the responsibility to conduct SIM card changes without sufficient oversight – as demonstrated by the representative and agent effectuating the October 2018 SIM swap on Mr. Ross' account despite AT&T's policy disallowing COAM SIM changes over the phone.

182. Additionally, as alleged fully above, the hacker involved in Mr. Ross' SIM swap had associated numerous different SIM cards with the same device IMEI in the days leading up to Mr. Ross' attack. Despite the highly suspicious nature of this activity, and AT&T's ability to track such requests, AT&T and its agents failed to put any additional protections on customer accounts to prevent its employees from approving additional SIM swaps to the same IMEI.

183. Upon information and belief, Defendants failed to exercise due care in selecting their agents and employees, and thereby negligently or recklessly employed employees to do acts—including accessing customer accounts and effectuating SIM swaps—which necessarily brought them in contact with others, including Mr. Ross, while in the performance of those duties.

184. Defendants' acts, as alleged herein, were negligent in that they created the risk of unauthorized account access, SIM card changes, and the damages resulting therefrom.

185. Defendants also failed to properly supervise their agents and employees, and instead continued to negligently entrust them with sensitive customer data. On information and belief, had AT&T not contracted out customer service functions to third parties such as One Touch Direct and One Touch Direct-SA, and had One Touch Direct or One Touch Direct-SA fired the involved the employee when they first began to exhibit suspicious SIM swap activity—including but not limited to approving SIM changes that violated AT&T policy—Mr. Ross would not have been injured.

186. On information and belief, had Defendants built a system to effectively authenticate and verify consumer consent before allowing its agents or employees to access their CPNI—as required by the FCA—Mr. Ross would not have been injured.

187. On information and belief, had Defendants prevented individual employees from unilaterally performing SIM swaps without proper oversight, Mr. Ross would not have been injured.

188. In sum, Defendants gave their agents and employees the tools and opportunities they needed to gain unauthorized access to Mr. Ross' account and failed to prevent them from doing so, thereby allowing them to use AT&T's systems to perpetuate privacy breaches and thefts against Mr. Ross.

189. The Defendants' agent(s') and employee(s') actions have a causal nexus to their employment. Mr. Ross' injuries arose out of his contract with AT&T as his carrier, and AT&T's access to his CPNI and account data as a result. The risk of injury to Mr. Ross was inherent in the AT&T working environment.

190. Mr. Ross' injury was also foreseeable. As alleged fully above, Defendants were aware of the risks that SIM swaps presented to AT&T customers. Defendants were also aware that AT&T customers' accounts were vulnerable to unauthorized access by their agents and employees, as demonstrated in the 2015 FCC enforcement action. Furthermore, Mr. Ross' injury was foreseeable as Defendants could have and should have seen that the same hacker phone had been used in multiple previous unauthorized SIM swaps.

**COUNT VI**

**Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030**

191. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

192. Mr. Ross' mobile device is capable of connecting to the Internet.

193. Defendants' agents and employees, in the scope of their employment, intentionally accessed Mr. Ross' mobile device, and assisted others in accessing his mobile device, without Mr. Ross' authorization, in order to assist hackers in their theft of Mr. Ross.

194. The Defendants agents and employees took these actions knowing that they would cause damage to Mr. Ross' mobile device, as well as damage to the information located on his mobile device.

195. The Defendants agents and employees caused Mr. Ross' mobile device and much of the data on it to be unusable to him.

196. Because of the Defendants' agents' and employees' actions, Mr. Ross suffered damage to his mobile device and damage to information on his mobile device, including being unable to access information and data on his mobile device

and being unable to access his personal accounts, including his personal (e.g. G-mail) and financial (e.g. cryptocurrency and PayPal) accounts.

197. The act of swapping Mr. Ross' AT&T mobile SIM card was in the scope of the Defendants' agents and employees' work.

198. Further, Mr. Ross spent in excess of $5,000 investigating who accessed his mobile device and damaged information on it.

## VII. PRAYER FOR RELIEF

199. WHEREFORE, Plaintiff Robert Ross requests that judgment be entered against Defendants and that the Court grant the following:

A. Judgment against Defendants for Plaintiff's asserted causes of action;

B. Public injunctive relief requiring cessation of Defendants' acts and practices complained of herein pursuant to, *inter alia*, Cal. Bus. & Prof. Code § 17200 and 47 U.S.C. § 401(b);

C. Pre- and post-judgment interest, as allowed by law;

D. An award of monetary damages, including punitive damages, as allowed by law;

E. Reasonable attorneys' fees and costs reasonably incurred, including but not limited to attorneys' fees and costs pursuant to 47 U.S.C. § 206; and

F. Any and all other and further relief to which Plaintiff may be entitled.

## DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues so triable.

DATED: August 25, 2020

CHRISTOPHER GRIVAKES
AFFELD GRIVAKES LLP

By: /s/
Christopher Grivakes
Attorneys for Plaintiff ROBERT ROSS